Записки научных
семинаров ПОМИ
Том 281, 2001 г.

А. В. Яковлев

О p–РАСШИРЕНИЯХ ПОЛЕЙ ХАРАКТЕРИСТИКИ p

1. Категория $\mathfrak{M}_{k,G}$. Пусть k – поле характеристики $p \neq 0$, G – конечная группа, $k[G]$ – групповая алгебра G над k. Далее, пусть $\Lambda_{k,G}$ – кольцо, порожденное $k[G]$ и элементом F, удовлетворяющим следующим определяющим соотношениям:

$$aF = Fa^p, \; gF = Fg \quad \text{для всех} \; a \in K, g \in G.$$

Обозначим через $\mathfrak{M}_{k,G}$ категорию правых $\Lambda_{k,G}$-модулей, конечно порожденных как $k[G]$-модули. Иными словами, любой объект M категории $\mathfrak{M}_{k,G}$ – конечно порожденный правый $k[G]$-модуль, рассматриваемый вместе с эндоморфизмом $x \rightsquigarrow x^F$ *аддитивной группы* модуля M, таким что

$$(xa)^F = x^F a^p, \; (xg)^F = (x^F)g \quad \text{для всех} \; a \in K, x \in M, g \in G.$$

Лемма 1. *В категории $\mathfrak{M}_{k,G}$ выполняется теорема Крулля–Шмидта.*

Действительно, каждый объект M этой категории является артиновым и нетеровым $\Lambda_{k,G}$-модулем, потому что M – конечномерное векторное пространство над k, и, тем самым, M является артиновым и нетеровым уже как модуль над кольцом $k \subseteq k[G] \subset \Lambda_{k,G}$.

Лемма 2. *Пусть G – p-группа, H – нормальная подгруппа G индекса p. Предположим, что объект M категории $\mathfrak{M}_{k,G}$ удовлетворяет условиям:*

(1) *как $k[G]$-модуль M изоморфен $k[G]$;*
(2) *ядро отображения $F - \mathrm{id}_M$ является группой порядка p.*

Тогда существуют H-инвариантный, но не G-инвариантный элемент $t \in M$, элемент $u \in M$ и элемент $a \in k$, такие что

Работа поддержана РФФИ, грант 01-01-00964.

$u^F = u \neq 0$, $ug = u$ для всех $g \in G$, $t^F = t + au$. Многочлен $z^p - z - a$ неприводим над k.

Доказательство. Обозначим ядро гомоморфизма $F - \mathrm{id}_M$ через A. По условию (2), порядок группы A равен p. Если $u \in A$, $g \in G$, то $(ug)^F - ug = (u^F - u)g = 0$, т.е. $ug \in A$. Следовательно, A – G-инвариантная подгруппа M; поскольку порядок A равен p, а G – p-группа, G тривиально действует на A. Выберем любой ненулевой элемент $z \in A$; поскольку M – свободный $k[G]$-модуль, а элемент u является G-инвариантным, существует такой элемент $x \in M$, что $u = x(\sum\limits_{g \in G} g)$.

Пусть g – какой-то элемент из G, не содержащийся в H; тогда

$$u = x \sum_{g \in G} g = x(\sum_{h \in H} h)(1 + g + \cdots + g^{p-1}) = x(\sum_{h \in H} h)(g-1)^{p-1}.$$

Пусть $t = x(\sum_{h \in H} h)(g-1)^{p-2}$; тогда $t(g-1) = u$. Поскольку, очевидно, $(g-1)\sum_{h \in H} h = \sum_{h \in H} h(g-1)$, мы получаем также, что $t = x(g-1)^{p-2}\sum_{h \in H} h$; следовательно, $th = t$ для всех $h \in H$. Далее,

$$(t^F - t)(g-1) = (t(g-1))^F - t(g-1) = u^F - u = 0;$$
$$(t^F - t)(h-1) = (t(h-1))^F - t(h-1) = 0 \quad \text{для всех} \quad h \in H,$$

откуда следует, что $v = t^F - t$ – G-инвариантный элемент. Но $k[G]$-модуль M изоморфен $k[G]$; поэтому любые два ненулевых G-инвариантных элемента из M различаются только множителем из k. В частности, существует такой элемент $a \in k$, что $au = v = t^F - t$.

Если бы многочлен $z^p - z - a$ был приводим над k, то у него был бы корень $b \in k$. Но тогда было бы $(t - bu)^F = t^F - b^p u^F = t + au - (b+a)u = t - bu$, т.е. элемент $t - bu$ принадлежал бы A и потому был бы G-инвариантным. Вместе с ним G-инвариантным был бы и элемент $t = (t - bu) + bu$. Но $tg = t + u \neq t$; это противоречие и доказывает последнее утверждение леммы 2.

2. Замена основного поля. Пусть l – расширение поля k, H – подгруппа G. Если M – объект категории $\mathfrak{M}_{k,G}$, то положим $M' = M \otimes_k l$ и следующим образом распространим на M' действие автоморфизмов из группы H и эндоморфизма F:

$$(m_1 \otimes_k b_1 + \dots + m_r \otimes_k b_r)h = m_1 h \otimes_k b_1 + \dots + m_r h \otimes_k b_r,$$
$$(m_1 \otimes_k b_1 + \dots + m_r \otimes_k b_r)^F = m_1^F \otimes_k b_1^p + \dots + m_r^F \otimes_k b_r^p,$$

(здесь r – произвольное натуральное число, $h \in H$, $b_1, \dots, b_r \in l$, $m_1, \dots, m_r \in M$). Соответствие $M \rightsquigarrow M'$ определяет функтор $\mathcal{P}_{l,H}^{k,G} : \mathfrak{M}_{k,G} \to \mathfrak{M}_{l,H}$.

3. Функтор $\mathcal{F}$. Пусть φ – изоморфизм поля k характеристики p на подполе поля K, такой что расширение $K/\varphi(k)$ – конечное расширение Галуа с группой Галуа G. Превратим K в объект категории $\mathfrak{M}_{k,G}$, взяв в качестве F эндоморфизм $x \to x^p$ аддитивной группы поля K и положив

$$x(\sum_{g\in G} a_g g) = \sum_{g\in G} \varphi(a_g)x^g \qquad (x \in K,\ a_g \in k).$$

Будем обозначать этот объект через $\mathcal{F}_k^{\varphi}(K)$. Если поле K само является расширением поля k и φ – тождественный изоморфизм, то мы будем опускать его в записи и обозначать соответствующий объект категории $\mathfrak{M}_{k,G}$ через $\mathcal{F}_k(K)$.

Лемма 3. *Пусть φ – изоморфизм поля k характеристики p на подполе поля K, причем $K/\varphi(k)$ – расширение Галуа с группой Галуа G. Тогда объект $M = \mathcal{F}_k^{\varphi}(K)$ категории $\mathfrak{M}_{k,H}$ удовлетворяет условиям* (1), (2) *леммы* 2.

Доказательство. Первое свойство эквивалентно существованию нормального базиса расширения Галуа $K/\varphi(k)$, а это хорошо известно. Второе свойство очевидно: если $a \in \operatorname{Ker}(F - \mathrm{id}_M)$, то $x^p - x = x^F - x = 0$, т.е. x принадлежит простому подполю $\mathbb{F}_p$ поля K.

Лемма 4. *Пусть φ – изоморфизм поля k характеристики p на подполе поля K, такой что $K/\varphi(k)$ – конечное расширение Галуа. Далее, пусть G – группа Галуа расширения $K/\varphi(k)$, H – нормальная подгруппа G и l – расширение k, для которого существует изоморфизм l на подполе K^H H-инвариантных элементов поля K, продолжающий вложение $\varphi : k \to K$. Тогда объект $\mathcal{P}_{l,H}^{k,G}(\mathcal{F}_k^{\varphi}(K))$ изоморфен прямой сумме $\bigoplus_{\psi} \mathcal{F}_l^{\psi}(K)$, где ψ пробегает множество* *всех изоморфизмов поля l на поле K^H, продолжающих вложение φ.*

Доказательство. Пусть $l = k(\zeta)$, где ζ – корень неприводимого многочлена $f(z) = a_0 + a_1 z + \cdots + z^n$ с коэффициентами из k. Обозначим через $\theta_1, \ldots, \theta_n \in K$ все корни многочлена $f^\varphi(z) = \varphi(a_0) + \varphi(a_1)z + \cdots + z^n$. Превратим K в k-модуль, положив $xa = \varphi(a)x$ для любых $x \in K$, $a \in k$. Как $k[G]$-модуль, объект $\mathcal{P}^{k,G}_{l,H}(\mathcal{F}^\varphi_k(K))$ совпадает с алгеброй $\Gamma = K \otimes_k l$, а действие эндоморфизма F совпадает с возведением элементов из Γ в p-ую степень. Элементы e_i, определенные формулой

$$\frac{(1\otimes\zeta\ -\theta_1\otimes 1)\ldots(1\otimes\zeta\ -\theta_{i-1}\otimes 1)(1\otimes\zeta\ -\theta_{i+1}\otimes 1)\ldots(1\otimes\zeta\ -\theta_n\otimes 1)}{(1\otimes\theta_i-\theta_1\otimes 1)\ldots(1\otimes\theta_i-\theta_{i-1}\otimes 1)(1\otimes\theta_i-\theta_{i+1}\otimes 1)\ldots(1\otimes\theta_i-\theta_n\otimes 1)},$$

являются попарно ортогональными идемпотентами алгебры Γ, и их сумма $e_1 + \cdots + e_n$ является единицей Γ.

Алгебра Γ раскладывается в прямую сумму идеалов $K_i = \Gamma e_i$; отображение $\alpha_i : K \to K_i$, заданное формулой $\alpha_i(x) = (x \otimes 1)e_i$, является изоморфизмом поля K на K_i, и очевидно, что этот изоморфизм сохраняет действие автоморфизмов из H и эндоморфизма F. Напротив, при $x \in K$, $a \in k$ мы имеем: $\alpha_i(x)a = (x \otimes 1)e_i a = (x \otimes a)e_i(x\varphi(a) \otimes 1)e_i = \alpha_i(x\varphi(a))$. В частности, при $x = 1$ получаем: $e_i a = (1 \otimes 1)e_i a = \alpha_i(\varphi(a))$, т.е. $\varphi(a) = \alpha_i^{-1}(e_i a)$. Продолжим отображение φ до отображения $\psi_i : l \to K$, заданного той же формулой: $\psi_i(b) = \alpha_i^{-1}(e_i b)$ для всех элементов $b \in l$. Отображение ψ_i представляет собой изоморфизм поля l на подполе поля K, и ясно, что $\psi_i(l) \subseteq K^H$. Но $(\psi_i(l) : \varphi(k)) = (l : k) = (K^H : \varphi(k))$; поэтому $\psi_i(l) = K^H$.

Покажем теперь, что α_i индуцирует изоморфизм объекта $\mathcal{F}^{\psi_i}_l(K)$ категории $\mathfrak{M}_{l,H}$ на прямое слагаемое K_i объекта

$$\mathcal{P}^{k,G}_{l,H}(\mathcal{F}_k(K)) = K \otimes_k l = \Gamma.$$

В самом деле, $\mathcal{F}^{\psi_i}_l(K) = K$ и действие операторов из группового кольца $l[G]$ определяется формулой

$$x(\sum_{h\in H} b_h h) = \sum_{h\in H} \psi_i(b_h)x^h \qquad (x \in K,\ b_h \in l).$$

Поэтому

$$\alpha_i(x(\sum_{h\in H} b_h h)) = \alpha_i(\sum_{h\in H} \psi_i(b_h)x^h) = \sum_{h\in H} \alpha_i\psi_i(b_h)(\alpha_i(x))^h =$$
$$= \sum_{h\in H} e_i b_h(\alpha_i(x))^h = \sum_{h\in H} b_h(\alpha_i(x))^h = (\alpha_i(x))(\sum_{h\in H} b_h h).$$

Соотношение же $\alpha_i(x^p) = (\alpha_i(x))^p$ очевидно.

Изоморфизм ψ_i отображает элемент $\zeta \in l$ в элемент $\theta_i \in K$; следовательно, $\psi_1, \dots, \psi_n$ – это все изоморфизмы поля $l = k(\zeta)$ на поле K^H, продолжающие вложение φ. Лемма 4 полностью доказана.

4. Главная теорема.

Теорема 1. *Пусть k – поле характеристики p и G – конечная p-группа. Пусть K, L – расширения Галуа поля k с группой Галуа G. Если объекты $\mathcal{F}_k(K)$, $\mathcal{F}_k(L)$ категории $\mathfrak{M}_{k,G}$ изоморфны, то и поля K, L изоморфны.*

Доказательство. На самом деле мы будем доказывать индукцией по порядку $|G|$ группы G немного более сильное утверждение.

Теорема 1$'$. *Пусть φ, ψ – изоморфизмы поля k характеристики p на подполя полей K, L. Предположим, что $K/\varphi(k)$, $L/\psi(k)$ – расширения Галуа с группой Галуа G. Если объекты $\mathcal{F}_k^{\varphi}(K)$, $\mathcal{F}_k^{\psi}(L)$ категории $\mathfrak{M}_{k,G}$ изоморфны, то существует такой изоморфизм полей $\mu : K \to L$, что $\mu\varphi = \psi$.*

Если $|G| = 1$, то $K = \varphi(k)$, $L = \psi(k)$, и наше утверждение бессодержательно. Предположим, что теорема уже доказана для всех полей k и всех групп меньшего порядка. Выберем в группе G нормальную подгруппу H индекса p; пусть K^H, L^H – поля H-инвариантных элементов полей K и L.

Пусть M – объект категории $\mathfrak{M}_{k,G}$, изоморфный $\mathcal{F}_k^{\varphi}(K)$ и $\mathcal{F}_k^{\psi}(L)$. Лемма 3 показывает, что объект M удовлетворяет условиям (1), (2) леммы 2; поэтому найдутся H-инвариантный, но не G-инвариантный элемент $t \in M$, элемент $u \in M$ и элемент $a \in k$, такие что $u^F = u \neq 0$, $ug = u$ для всех $g \in G$, $t^F = t + au$. Пусть l – поле разложения неприводимого над полем k многочлена $z^p - z - a$; хорошо известно, что поле l можно получить присоединением к полю k лишь одного корня этого многочлена ζ. Объект $\mathcal{F}_k^{\varphi}(K)$ изоморфен M; поэтому существуют G-инвариантный элемент $u_0 \in K$, H-инвариантный, но не G-инвариантный элемент $t_0 \in K$ и элемент $a \in k$, такие что $u_0^p = u_0^F = u_0$, $t_0^p = t_0^F = t_0 + \varphi(a)u_0$. Элемент $\eta = t_0/u_0 \in K$ H-инвариантен, но не G-инвариантен, и он удовлетворяет уравнению $\eta^p = (t_0/u_0)^p = t_0^p/u_0^p = (t_0 + \varphi(a)u_0)/u_0 = \eta + \varphi(a)$. Поэтому мы можем единственным образом продолжить φ до изоморфизма φ_1 поля l на поле K^H, такого что $\varphi_1(\zeta) = \eta$. Аналогично показывается, что существует изоморфизм l на L^H, продолжающий вложение $\psi : k \to L$.

Поскольку объект M изоморфен $\mathcal{F}_k^{\varphi}(K)$ и $\mathcal{F}_k^{\psi}(L)$, объект $\mathcal{P}_{l,H}^{k,G}M$ изоморфен объектам $\mathcal{P}_{l,H}^{k,G}(\mathcal{F}_k^{\varphi}(K))$, $\mathcal{P}_{l,H}^{k,G}(\mathcal{F}_k^{\psi}(L))$; по лемме 4, эти последние объекты изоморфны прямым суммам $\bigoplus_{i=1}^p \mathcal{F}_l^{\varphi_i}(K)$, $\bigoplus_{j=1}^p \mathcal{F}_l^{\psi_j}(L)$, где $\varphi_1, \ldots, \varphi_p$ – все изоморфизмы l на K^H, продолжающие φ, а $\psi_1, \ldots, \psi_p$ – все изоморфизмы l на L^H, продолжающие ψ. Поскольку теорема Крулля–Шмидта справедлива в категории $\mathfrak{M}_{l,H}$ (лемма 1), мы получаем, что эти два разложения изоморфны; в частности, существуют такие изоморфизмы $\varphi' = \varphi_i$ и $\psi' = \psi_j$ поля l на K^H и L^H, что $\mathcal{F}_l^{\varphi'}(K)$ и $\mathcal{F}_l^{\psi'}(L)$ – изоморфные объекты категории $\mathfrak{M}_{l,H}$. Но $|H| < |G|$, и, по предположению индукции, существует изоморфизм $\mu : K \to L$, такой что $\mu\varphi' = \psi'$. Так как ограничения φ', ψ' на k равны соответственно φ и ψ, из предыдущего соотношения следует, что $\mu\varphi = \psi$. Теорема $1'$ полностью доказана.

Yakovlev A. V. On p-extensions of fields of characteristic p.

It is proved that a p-extension of a field of characteristic p is completely defined by its Galois group and the endomorphism of the additive group of the group algebra, which corresponds to the raising in the power p.

С.-Петербургский
государственный университет
E-mail: yakovlev@yak.pdmi.ras.ru

Поступило 28 октября 2001 г.